(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 651 357 A1**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: 94306834.6

(51) Int. Cl.⁶: G07F 7/12

(22) Date of filing: 19.09.94

(30) Priority: 29.10.93 GB 9322360

(43) Date of publication of application: 03.05.95 Bulletin 95/18

(84) Designated Contracting States: DE FR GB

(71) Applicant: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504 (US)

(72) Inventor: Holloway, Christopher James
13 Wilders Close
Woking,
Surrey GU21 3HA (GB)

(74) Representative: Lloyd, Richard Graham
IBM (UK) Ltd,
UK Intellectual Property Department,
Hursley Park
Winchester,
Hampshire SO21 2JN (GB)

(54) **Transaction processing system.**

(57) A transaction processing system comprises at least one transaction terminal (10, 11, 12) having means to receive characteristic data from a user, which characteristic data is required to generate a characteristic image associated with the user, such as an image of the user's signature, from data stored in a data processing system (14); and logic for generating a transaction message by combining transaction data with the characteristic data in such a way that the transaction data is required to recover the characteristic data from the message. The data processing system (14) comprises means to store the user data, to receive and store the message, to recover the characteristic data from the message using the transaction data, and to reconstruct the characteristic image from the user data using the characteristic data to establish that the transaction was valid by associating the characteristic image with the transaction data.

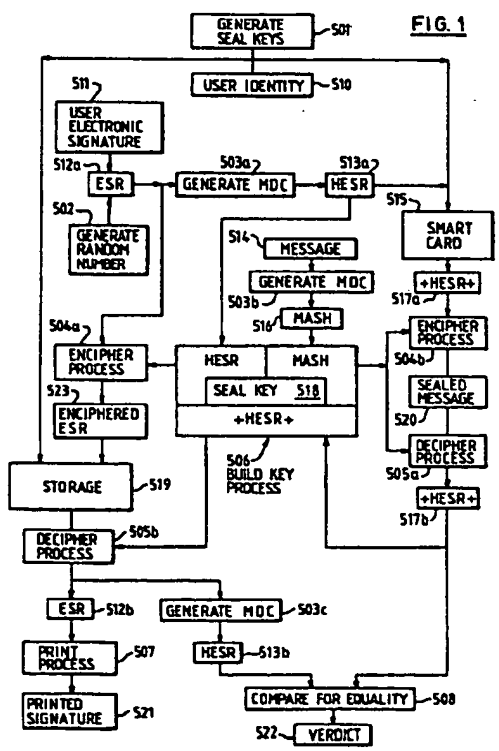


FIG. 1

EP 0 651 357 A1

This invention relates to security in transaction processing systems and, mor particularly, to the secure auth rization f transactions in transaction processing systems.

Examples of transaction processing systems include electronic point of sale (EPOS) systems allowing customers to pay for goods by means of credit cards or the like. Such a system includes one or more transaction terminals, at which details of a transaction and of a customer's card are entered, connected via a suitable data communications network to a data processing system storing, for instance, the customers' account details to effect a transaction in the customer's account.

The fraudulent use of such systems is a serious problem which in 1991 resulted in losses of 160 million pounds in the United Kingdom alone. Much effort is being invested in studying ways of addressing these huge losses.

Currently, transactions are usually authorized by recording the customer's signature on paper. This is because the signing of a name by an individual is a dynamic action which occurs in a remarkably repeatable fashion.

However, this traditional approach has a number of attendant problems. For example, it represents a tremendous burden to the merchant, who wants to get rid of paper, and certainly avoid the obligation of having to go back in his records in case of query to find a particular sales voucher with a signature on it.

The usage of other biometrics, such as the use of fingerprint or voice recognition, which can be verified using suitable apparatus is being considered as a way of recording the fact that a customer has authorized a transaction. However, in some countries the matter is complicated by the legal need to capture the signature as evidence of the transaction.

It is therefore desirable to use electronic copies of signatures as a means of allowing a customer to authorise a transaction.

However, any means of transferring signatures in electronic form, whether or not encrypted, yields them vulnerable unless a mechanism is provided for preventing an electronic signature from being associated with transactions other than the original that was authorised.

Furthermore, if the signature associated with a transaction needs to be captured, electronically transmitted and stored in such a way that an image of the signature can be reproduced as desired, then data communications and storage become a significant overhead.

This invention aims to improve security in transaction processing systems by solving these problems. This is achieved through a new approach to associating a us rs authority, manifesting itself in a printable characteristic imag , particularly, but not exclusively, a signature image, with a transaction authorised by the user.

Accordingly, a first aspect of the invention enables a transaction processing system to be provided comprising a data processing system and at least one transaction terminal for use at a remote location by a user, the transaction terminal comprising means to receive characteristic data from the user, which characteristic data is required to reconstruct a characteristic image associated with the user from user data stored in the data processing system; logic for generating a transaction message by combining data relating to a transaction with the characteristic data in such a way that the transaction data is required to recover the characteristic data from the transaction message; and means connectable to a data communications network for transmitting the transaction message to the data processing system, and the data processing system comprising: means to store the user data; means to receive from the network and store the transaction message; logic for recovering the characteristic data from the stored transaction message using the transaction data; and logic for reconstructing the characteristic image from the user data using the characteristic data for use in establishing that the transaction was valid by associating the characteristic image with the transaction data.

A transaction makes use of a piece of characteristic data which removes the need to capture or transmit image data with the transaction. This characteristic data is cryptographically bound to a particular transaction and so cannot be transferred or associated with another transaction. The characteristic data provides the recipient of the transaction with the ability and authority to associate a centrally held copy of the original image to the transaction data.

Thus, no image capture device is required at the transaction terminal and the overhead of transferring image data with the transaction is avoided. The fact that the transaction data is required to recover the characteristic data from the transaction message means that the characteristic data is inextricably linked to the transaction and cannot be associated with transactions other than the one intended.

Preferably, the transaction terminal comprises means to establish that the user is authorized to effect the transaction in order that the merchant may satisfy himself that the customer is bona fide. Thus, user verification can proceed on the basis of a Personal Identification Number (PIN) ntered by the user at the transaction terminal, biometric or other method chosen and checked at the transaction terminal.

Th transaction terminal can comprise a smart card supplied by the user and a smart card reader, the smart card comprising means to store the characteristic data and logic for combining the characteristic data with the transaction data for use in generating the transaction message. Preferably, the smart card comprises means for storing a user-specific encryption key and logic for encrypting the characteristic data using the user-specific encryption key. In this event, the data processing system also needs to use the user specific key to recover the characteristic data from the transaction message. This has security advantages because, without knowledge of the key, the characteristic data cannot be extracted from the smart card or the message decrypted if intercepted.

In one embodiment the user data comprises a random number combined with a digital representation of the signature and the characteristic data is generated from the user data using a hashing algorithm. This ensures that neither the characteristic data nor a clear copy of the signature can be used to generate a copy of the user data.

If desired, signature capture can also continue on paper as today, but it is only possible to reproduce the copy of the centrally held signature in association with a valid and authorised transaction.

Advantageously, the data processing system comprises a first data processing facility for use by a verifier which receives and stores the transaction message and effects the transaction using the transaction data; and a second data processing facility for use by an arbiter which, if necessary, can recover the characteristic data from the stored transaction message using the transaction data and reconstruct the characteristic image from the characteristic data to establish that the transaction was valid by associating the characteristic image with the transaction data.

In this embodiment, an authority called an "arbiter", can be appointed, who would be independent of the verifier, to be involved in "proving" the transaction by reconstructing the signature image in the event of a dispute regarding the validity of a claimed transaction.

In addition, the "verifier" can use the characteristic data to verify the validity of a transaction by storing an encrypted form of the user data encrypted using the characteristic data. On receiving the message the characteristic data can be recovered by the verifier from the stored transaction message using the transaction data, the encrypted user data decrypted using the recovered characteristic data, the characteristic data generated from the decrypted user data and compared with the recovered characteristic data to establish the validity of the transaction.

The invention also provides a transaction terminal adapted for use in the above described transaction processing, a smart card adapted for use in the transaction terminal, and data processing systems for use by the verifier and arbiter.

Also provided is apparatus for enrolling users of the transaction processing system, the apparatus comprising: means to generate and store a digital representation of the characteristic image for each user; and logic for generating the user data and the characteristic data from the digital representation of the characteristic image. In one embodiment, the apparatus comprises logic for encrypting the user data using the characteristic data and for creating the necessary encryption keys.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic diagram of the process of the preferred embodiment in its entirety;

Fig. 2 is the portion of Fig. 1 which relates to the enrolment process;

Fig. 3 is the portion of Fig. 1 which relates to the transaction process;

Fig. 4 is the portion of Fig. 1 which relates to the verification or validation process;

Fig. 5 is the portion of Fig. 1 which relates to the proving process;

Fig. 6 shows an implementation of a Seal Key Generating Service using as an example a particular choice of architecture, the IBM Common Cryptographic Architecture/1 (CCA/1);

Figs 7A to E show an implementation of a Seal Processing Service using the IBM CCA/1, and

Fig. 8 shows an example of transaction processing apparatus according to an embodiment.

A transaction processing system according to a simple embodiment of the invention takes the form shown in Fig. 8. A user provides details of a transaction at a transaction terminal 10, 11, 12, which could be, for example, a Point of Sale terminal provided in a shop to allow customers to initiate transfer of funds for the purchase of goods. Transaction data is transmitted to a data processing facility 13 storing users' details, which an authority called a verifier, a bank in this example, may use to validate the transaction. An arbiter may be used to prove the validity of a transaction in the event of a dispute, and in this case the transaction processing system would include a data processing facility 14 for the arbiter's use.

Broadly, the method of operation has four steps: enrolling, transacting, verifying or validating, and proving.

During enrolment, a copy of the signature is captured and stored securely in encrypted form by the verifier for future use. Data required to release the centrally stored signature is stored securely on

a card held by th user which is equipped with an integrated circuit chip containing a microprocessor and data storage faciliti s. Such cards are well understood in the art and have become known as 'smart cards'. The user held smart card also stores suitable program code and an encryption key which it shares with the verifier, and also with the arbiter if this option is taken.

The user uses his smart card to authorise a particular transaction at the transaction terminal. The terminal formulates the transaction data, and the microprocessor on the smart card appends to this data a seal. The seal combines cryptographically the data authorising release of the centrally stored signature with transaction data, and authenticates the message containing both the transaction data and the seal. The encryption makes use of the encryption key provided both to the smart card and to the verifier.

The verifier receives the transaction message and recovers the authority to use the stored signature. This authority is then used to establish that the signature data forming part of the seal, which is bound to the transaction, corresponds to the stored signature. Only if the correspondence is proven will the transaction be allowed to proceed. The verifier stores the original transaction message as evidence of the transaction in case any query should arise.

The step referred to as "proving" is invoked in the case of a dispute regarding the validity of a transaction. The original transaction message is processed using the shared encryption key and stored signature. The correspondence is demonstrated again, but this time in addition a clear copy of the stored signature is generated for printing together with the transaction data. The stored signature is constructed in such a way that the clear signature cannot be used to create an alternative stored signature which might be associated with another smart card user or transaction.

If it is decided to use an independent arbiter to prove the validity of a transaction in the event of a dispute, the enciphered signature is lodged with the arbitration authority enciphered under a key that allows the arbiter, but not the verifier, to print the clear signature. Thus only the arbiter would be able to perform the proving step. In the absence of an arbiter, the verifier would be able to perform this step.

Fig. 1 is a schematic diagram showing these steps. This diagram is reproduced in part in four further figures, Figs. 2 to 5, each covering one aspect of the process as described in further detail below.

Encryption algorithms allowing sensitive data to be protected, for example during electronic transmission, are widely known in th art and embodied in many systems. One such system is IBM's Transaction Security System, a set of hardware security products including a smart card and supporting the "Data Encryption Algorithm" (DEA). The DEA is a widely known algorithm, described for example in the book "Cryptography: A New Dimension in Computer Data Security" by Carl H. Meyer and Stephen M. Matyas, John Wiley & Sons 1982. The DEA was adopted by the US National Security Agency and National Bureau of Standards in 1977 as a federal standard.

Enrolling

As shown in Fig. 1, and Fig. 2, an encryption key called a "seal key" 501 is created and stored both in the verifier's storage 519 and on a smart card 515. Where the arbiter option is taken, a copy of the same key is provided to the arbiter who may use it for obtaining the clear signature to print. The seal key is specific to each user and is stored together with data on the user's identity 510 which will allow the appropriate seal key to be retrieved from the verifier's or arbiter's storage when required.

In IBM's Transaction Security System the usage of encryption keys may be controlled by associating with each key a Control Vector which defines its permitted usages, and this definition is enforced within the security hardware device itself. Such a Control Vector mechanism, or similar, is used to enforce the different usages of the two or three manifestations of this key. In the description which follows the seal key is referred to as a Sealing Key when used by the smart card, as a Seal Verification Key when used by the verifier and as a Seal Proving Key when used for proving by the arbiter, or in the absence of an arbiter by the verifier. Each of the types of seal processing key is represented in the diagrams by the seal key 518, irrespective of its individual function.

The user receives the smart card 515 and authenticates himself to the verifier authority using whatever means of personal authentication is appropriate, such as a Passport, driving licence etc. The user enrols by providing a means of electronic authentication which can be performed at the transaction terminal by the smart card itself or the smart card in combination with the transaction terminal. This might be a PIN, password, signature, finger print, facial image, retina pattern etc. The reference pattern for this authentication would be stored on the smart card and would be used, in a conventional manner, to authorise the smart card to process a transaction as described below.

In addition, the user also registers a copy of his handwritten signatur which is captured in the form of a reproducible image 511. The imag cap-

ture and printing technology is not described here but is conventional and will be well understood by the person skilled in the art. The electronic form of the signature image is a binary string of indefinite length which is padded with binary zeros (white space) to the nearest eight byte boundary point. It may also have associated with it control information describing how to reconstruct the signature from the electronic image, and it may have been compressed. This construct will be referred to as the "electronic signature" 511.

The electronic signature is preceded with a generated random number 502 (RNA) to form an "electronic signature record" or ESR 512a. Note that where reference figures are followed by a suffix eg. 512a, 512b these denote occurences at different points in the diagram of the same data value or same process. The RNA is an arbitrary binary string of at least eight bytes, and preferably 8 or 16 bytes, since 8 bytes is a sufficient minimum for cryptographic strength, and working on 8 byte boundaries avoids the need for further padding. This use of the random number RNA prevents any copy of the clear electronic signature, or a copy of the handwritten signature, from being used to create a replica signature block to be wrongly associated with any other already issued smart card.

The whole ESR 512a is reduced to a relatively short length using a "hashing" algorithm, such as the algorithm MDC2 implemented in the IBM Transaction Security System. A detailed description of the MDC2 algorithm is given in an article by S. M. Matyas, "Key handling with control vectors", IBM Systems Journal 30, No. 2, 151-174 (1991), and available from IBM as Reprint Order No. G321-5428. The MDC2 algorithm is a "modification detection code" based on DEA encryptions. A modification detection code is a nonsecret cryptographic variable of fixed, relatively short length calculated from a message with a public (nonsecret) one-way function. A cryptographic one-way function has the property that, given the output, cryptographic key, and algorithm, it is impractical to derive the input value, or to derive another input resulting in the same output. The MDC2 algorithm processes data in multiples of 8 bytes, with a 16 byte minimum and results in a 16 byte output.

The MDC2 algorithm is therefore suitable for reducing the ESR 512a, which in this embodiment is of indefinite length, and results in a hashed ESR (HESR 513a), an arbitrary binary string of 16 bytes which is specific to the electronic signature and associated random number RNA.

The HESR, or a function of the HESR is then used to encipher 504a the value of the ESR 512a. This enciphered ESR 523 is stored in the verifier's storage 519, together with any necessary data, eg. a user or smart card number, to allow it to be retrieved and associated with the correct user. Th HESR 513a, or th function thereof, is stored in th memory of the smart card for use when transacting, but is not stored elsewhere in the system.

In this embodiment, the encipher process 504a selected is a "triple encipherment" process, but other enciphering methods known in the art could be used. Triple encipherment is a process defined in IBM's Common Cryptographic Architecture/1 (CCA/1), which is implemented in the IBM Transaction Security System previously mentioned. The 16 byte HESR 513a is first combined with the 16 byte seal key 518 via the Build Key Process 506. The Build Key Process could be, for example, a simple exclusive OR operation, or if desired an encryption. The resulting 16 byte key is then used as a "double length DEA key" to triple encipher the ESR 512a. The triple encipherment entails splitting the 16 byte key into 8 byte left and right halves, DEA enciphering with the left, DEA deciphering with the right, and finally DEA enciphering with the left half.

The use of the HESR 513a to encipher the ESR 512a for storage by the verifier prevents the verifier from deciphering the stored and enciphered signature 523 without the HESR 513a information, which is obtainable only from the smart card 515. In other words, the verifier is not able to obtain the deciphered signature without the authorisation of the smart card 515 user.

Transacting

The transaction portion of the process is shown in Fig. 3. A transaction is established and agreed upon at a transaction terminal. This manifests itself as a formatted and structured bit string or character string coded in binary and is called a "message" 514. The message contains time variant information and terminal specific information so that it may be uniquely identified; as well as details of the transaction itself. To perform the transaction the user authenticates himself at the transaction terminal using his smart card 515 and whatever means of electronic authentication has been adopted. This authentication also indicates the user's agreement to the transaction.

Having authenticated the user, the smart card receives the message, appends smart card specific data to allow the card and the user to be identified, and creates a seal using the process described below. This seal is appended to the message to form a "sealed message" 520. It will be understood that the whol sealed message may be authenticated by calculating check digits, such as a Message Authentication Code (MAC), or Digital Signature (DSG); but this would be an independent process, and is not described her as appropriate

methods are well known in the art.

The sealed message 520 comprising message 514, smart card data, and seal is transmitted to the verifier.

The process for generating the seal is closely analogous to the process for generating the enciphered electronic signature stored by the verifier. Thus the seal is calculated as follows:

The message 514 is a binary string of indefinite length which would be padded if necessary to the nearest 8 byte boundary. The message is subjected to a hashing algorithm to reduce it to a 16 byte binary string. This hashing algorithm could, but need not, be the one used to reduce the ESR 512a to the HESR 513a, for example the MDC2 algorithm. The resultant 16 byte binary string will be referred to as the Message Hash or MASH 516.

The hashing algorithm may use a default hashing key or, optionally, an arbitrarily generated hashing or "transaction key". If an arbitrarily generated key is used, this key must be transmitted to the verifier with the transaction message. Secure transmission of transaction or of MAC verification keys is well known in the art and is not discussed further here.

The Build Key Process 506 then combines the MASH 516 with the Sealing Key 518. In this embodiment both are 16 bytes and the Build Key Process 506 could be a simple exclusive OR operation, resulting in a 16 byte key. This key is then used as a double length DEA key to triple encipher 517a the HESR supplied from the card 515. This HESR read off the card will be denoted +HESR+ in the description and figures, since it is not assumed to be the same as the HESR recorded at enrolment; for example it may have been corrupted. The enciphered +HESR+, together with the hashing key, if required, is the seal. If a default hashing key known to the verifier is used rather than an arbitrarily generated one, then the hashing key need not be included.

The use of the binary string MASH 516, generated from the transaction data, prevents the seal from having the same external appearance on any two occasions. Moreover, since the verifier or arbiter cannot decipher the HESR supplied from the card without reconstructing the MASH from the message 514 part of the sealed message 520, the seal cannot be deciphered if appended to any other message 514. This prevents the signature from being associated with any transaction other than the authorised transaction.

It is important to realize that the sealed message 520 transmitted to the verifier comprises th messag 514, smart card specific data and th seal. The seal alone is not sufficient to regenerate the full transaction message 514, since it is based on the sh rter MASH 516.

Validating

The verifier performs the following steps, shown in Fig. 4, to validate the transaction:

The binary string MASH 516 is calculated from the message portion 514 of the received sealed message 520 using the hashing algorithm which is also known to the verifier.

Using the MASH 516 and the Seal Verification Key 518 the verifier reconstructs via the Key Build Process 506 the double length key which was used to encipher the smart card stored +HESR+ 517a. The double length key is used to decipher 505a the +HESR+ 517b from the seal portion of the sealed message 520. In other words, the message portion 514 containing transaction details is needed in order to decipher 505a the +HESR+ 517b. If the seal becomes associated with a message 514 other than the authorised one used in the creation of the seal, it will be impossible to derive the +HESR+ 517b.

The smart card specific data, such as a smart card or user number, received as part of the sealed message 520 is used by the verifier as an index to retrieve the enciphered ESR corresponding to that user from storage 519.

The +HESR+ 517b is then used to decipher 505b the stored enciphered ESR 523. To do this, the +HESR+ 517b is combined with the Seal Verification Key 518 via the Build Key Process 506, and then used to reverse the triple encipher process 504a which was applied to the ESR 512a prior to storing 519 it. The clear value of the electronic signature ESR is thus obtained as an intermediate step at this point, but is not otherwise disclosed.

Next, the ESR is hashed 503c to generate a HESR value 513b of the result, since it is desired to compare the verifier's stored signature information with the smart card stored value, +HESR+, which is of the hashed form. In the preferred embodiment, the hashing process which is here applied to the signature stored by the verifier is identical to that used to generate the HESR stored on the smart card.

The verifier compares 508 this HESR 513b generated from the stored enciphered signature 523 with the recovered +HESR+ 517b from the message. A verdict 522 is given of the integrity of the received message. In the embodiment described, the comparison 508 is for equality, since identical hashing processes 503a, 503c were used. It will be understood that, if non-identical hashing processes were used, the comparison would not be for equality, but would need to be based on a functional relationship between the hashing processes.

Thus the signatur 523 stored by the verifier, once deciphered and hashed, is verified against the

quoted HESR valu +HESR+ 517b used to decipher it. If the tw signatures do not match, the deciphering process will not actually yield the true ESR valu . The true HESR value obtainabl only from the smart card is necessary to allow the verifier to decipher the signature.

A receiving application should also perform validation of the transaction contents not described here. If the message was authenticated with further check digits such as a MAC or DSG, these would also be verified.

Proving

The proving part of the process is shown in Fig. 5. During a dispute about the validity of a particular transaction, the verifier, or the arbiter (if appropriate), performs the same set of steps as described above, using a copy of the sealed message 520 stored at the time of the transaction. This time, however, the random number RNA is also stripped from the ESR 512b, and the electronic signature 521 is disclosed 507 and printed along with the transaction data in a suitable form.

The ability to reproduce the printed signature in association with the transaction establishes that the user's authority was granted and that the genuine smart card, holding the Sealing key 518 and HESR value 513a, was used to authorise the transaction.

It would be possible to use more than one seal key; one key shared between the smart card and the verifier could be used for enciphering 504b and deciphering 505a the seal, while another key could be used to encipher 504a and decipher 505b the stored signature information. Other alternatives to the specific encryption schemes and algorithms described, which are based on encryption methods known in the art, could be used. The bit lengths of variables could be changed without affecting the essence of the invention.

However, it is significant that the verifier alone is unable to reconstruct the unencrypted ESR, but requires information supplied from the smart card to decrypt his copy. Another significant feature is that the signature cannot be associated with a transaction other than the authorised transaction. This is achieved in the preferred embodiment by means of a particular seal or encryption scheme using algorithms known in the art; clearly other alternatives which preserved this feature could be used. Finally, such a scheme could if desired be applied to data other than signature data, such as, for example, a photograph; signature data is used as an example due to the legal status of the signatur in many countries.

Implementation in the IBM Common Cryptographic Architecture/1

Although the above d scription is detailed enough to allow the invention to be implemented, it will now be described how the invention could be implemented using a particular architecture, IBM's Common Cryptographic Architecture/1, described in the manual "Cryptographic API Interface Reference", Order No. SC40-1675-01 available from International Business Machines Corporation. IBM's Transaction Security System is an example of a system using this architecture.

In the IBM Common Cryptographic Architecture/1, each encryption key has its usage defined by a Control Vector (CV). A CV is a structured 128 bit binary string whose value determines how the key may be used. Secure cryptographic hardware, such as can be found in the IBM Transaction Security System, interprets the control vector and enforces the usage constraints.

When encryption keys are transferred between cryptographic units, they are enciphered using higher level keys called key encrypting keys (KEKs). Before encipherment the KEK is modified by exclusive OR with the CV of the key being transferred. At the receiving unit the correct key will be deciphered only if the CV has not been corrupted in transit. Keys stored outside of secure hardware for local use are also enciphered by a KEK modified by the key's CV.

The KEKs are of three principle types (there are other types of no relevance here). A MASTER key is stored inside the secured hardware and is not shared with any other device. A key stored enciphered under a MASTER key is ready to be presented to the device which internally deciphers the key into clear form ready for use. To exchange keys between devices a shared KEK is required: this one KEK is known as an EXPORTER to the sending device and as an IMPORTER to the receiving device, although the key itself has the same value. The difference is in usage as defined by the different CVs at each device.

In this embodiment, such shared Key Encrypting Keys, defined to be IMPORTER/EXPORTER pairs, are generated and exchanged between the Arbiter and the Verifier, and between the Smart Card and the Verifier in an initial setup step. In both cases the EXPORTER form is held by the Verifier, and indicated in Fig. 6.

These key pairs are as follows:

- KKEXPcrd 201 held by the verifier and its counterpart KKIMPcrd held by the card, and
- KKEXParb 202 held by the verifier and its counterpart KKIMParb held by the arbiter.

The purpose of this initial setup step is to provide shared Key Encrypting Keys to secure the

subsequent exchange of a seal key.

Using a "Key Generate" service a device can create a key already enciphered under the appropriate KEK (MASTER ready for use; IMPORTER ready to receive back to itself; EXPORTER ready to send). The selection of KEK type for output from Key Generate is called the Key Form, and is designated EX for EXPORTER, IM for IMPORTER and OP (meaning Operational form) for MASTER.

The Key Generate Function in CCA/1 outputs one or two key forms. For this embodiment a new Hey Generate Service 200 is defined, extending Key Generate to provide three outputs as shown in Fig. 6. Thus a single key, the Seal Key part 1 215 in Fig. 6, is generated 211 and output in three forms 220, 221, 222. This is achieved by enciphering 214 the Seal Key Part 1 215 under each of the KEKs 201, 202, 203 in turn, but in each case the KEK which is stored enciphered under a MASTER key 210 is first deciphered 212 using the MASTER key 210 and then exclusively ORed 213 with a different CV 216 based on the purpose of the key.

A Control Word 204 on the Service Call API (Application Programming Interface) allows the Key Form to be specified. In this embodiment either EXEXOP or EXEXIM is selected, where EXEXIM, for example, means the three forms of KEK 201, 202, 203 must be EX, EX and IM respectively. IMPORTER 203 is needed only if the EXEXIM control word is chosen; the creation and provision of a local IMPORTER key is not described here. If EXEXOP is selected, the MASTER key 210 is used and is already in the secure hardware boundary. The MASTER KEY 210 is used to decipher 212 each KEK internally so that it can be used; it will also be used to encipher 214 the Seal Key Part 1 to produce the Seal Verification Key 222 if EXEXOP is selected.

The "1" in Seal Key Part 1 215 is intended to indicate that this is the first component of a partial key, and so should not be used until after the key build process has completed.

The three forms of the Seal Key are

- A Sealing Key 220 enciphered under the EXPORTER EXPKEK(crd) 201 shared with the card
- A Seal Proving Key 221 enciphered under the EXPORTER EPKEK(arb) 202 shared with the arbiter
- A Seal Verification Key 222 enciphered under the Master Key 210 of the verifier, or under a local IMPORTER key, IMPKEK(enr) in Fig. 6.

The Sealing Key 220 and the Seal Proving Key 221 are imported at the smart card and the arbiter respectively under the appropriate IMPORTER keys, IMPORTER IMPKEK(crd) and IMPORTER IMPKEK(arb). The Seal Verification Key 222 is for local use by the verifier.

The Control Vector definitions are extended such that the Seal Verification key 222 cannot be used in a function which discloses a clear signature; but the Seal Proving key 221 may be. In all three cases the control vector defines the key to be a partial key only; that is it is incomplete without a final key part being combined with it. The process for combining these key parts is undefined here but could be a simple exclusive OR operation as the external interfaces to the secure services do not allow a user control over the value of either part. This is the Key Build Process 111a and 111b of Fig. 7.

Fig. 7 proposes an additional CCA/1 service, a Seal Processing Function 100, which can be used in different ways depending upon the settings of the input parameters Control Word 107. Hashing Key 106 determines whether a hashing key 103 is to be used. If not, MDC defines a default key to be used in the hashing or MDC algorithm. Only four of the possible combinations are relevant to this application.

Control Word 107 states whether the function is to Seal, as at enroller or on smart card, Verify or Prove.

The process for encrypting the signature ESR for storage at the time of enrolment will now be described. The key used to encrypt the ESR for storage is the Seal Verification Key 222 combined via the Key Build Process 111a with the HESR. As mentioned the Key Build Process 111a could be a simple exclusive OR operation. To perform this process using the Seal Processing Function 100, the electronic signature record ESR is presented as Input Data 1 101. The MDC process 110 proceeds with a hashing key 103 or the default key as determined by the hashing key Y/N 106. The HESR is then combined via the Key Build Process 111 with the Seal Verification Key 222 which is presented as Seal Key 104. The key thus produced is used to encipher 112a Input Data 1 102, which is the ESR value. The selection of the Data Input 1 101 to encipher 112a, and of encipherment rather than decipherment 112a is achieved by setting the Control Word 107 to ENROL. The enciphered ESR, represented as Output Data 3 123 is copied to the arbiter in this form. The completed key is not stored at any one location, but always rebuilt for usage from one of the three forms of the seal key and the HESR value.

The key used to encrypt the smart card stored HESR for transmission with a particular transaction message is obtained by calculating a 16 byte MDC over the message, input as Input Data 1 101 optionally using the arbitrary k y 103, as determined by the hashing key Y/N 106 setting, and combining this with the stored Sealing Key 220 which is presented as input 104 to the Key Build Process

111a. The smart card stored HESR is presented as Data Input 2 102 to the same function for encipherment 112a using this composit key, and th enciphered form is output as Data OUptu 3 123. To control this process, the Control Word 107 is set to SEAL, which determines the use of encipher as opposed to decipher internally 112 and the encipherment of Data input 2 102.

Validation and proving proceed in essentially the same way as each other. In both of these cases Input Data 1 101 is the received message 514, Data input 2 102 is the seal from sealed message 520 and Data input 3 103 is the stored enciphered ESR 523. For validation, input 104 the Control Word 107 is set to VERIFY to yield a good/bad result as Output Data 2 122 from the comparison process 113. For proving the Control Word 107 is set to 'PROVE', then in addition the clear electronic signature is released as Output Data 1 121. The printable signature output data 1 121 will be recognizable only if the verdict of Output data 2 122 is 'good'.

Thus the one API level service should invoke one of four lower level and independently controlled services for ENROLLING at the Verifier (107 = ENROL), SEALING on the smart card (107 = SEAL), VERIFYING (107 = VERIFY) and PROVING (107 = PROVE). The enrolling and verifying processes are enforced by the same CV, the sealing and proving processes are each enforced by other distinct CVs.

This embodiment is in line with the principles of the IBM Common Cryptographic Architecture/1. In particular, the usage of all keys is governed by Control Vector settings enforced by the cryptographic hardware; and all externally manifest keys are enciphered either under a Key Encrypting Key 201, 202, 203 for transportation and local storage; or under a hardware stored Master key 114, 210 for local use.

In Fig. 1 to Fig. 5 the three manifestations of the Seal Key are not distinguished; all are indicated as Seal Key 518.

Claims

1. A transaction processing system comprising a data processing system (14) and at least one transaction terminal (10, 11, 12) for use at a remote location by a user, the transaction terminal comprising means to receive characteristic data (517a) from the user, which characteristic data is required to generate a characteristic image associated with the user (521) from user data (523) stored in the data processing system; logic for generating a transaction messag (520) by combining data relating to a transacti n (514) with the characteristic data (517a) in such a way that the transaction data (514) is required to r c ver the characteristic data (517a) from the transaction message (520); and means connectable to a data communications network for transmitting the transaction message (520) to the data processing system,
and the data processing system comprising:
means to store the user data (523); means to receive from the network and store the transaction message (520); logic for recovering the characteristic data (517b) from the stored transaction message (520) using the transaction data (514); and logic for reconstructing the characteristic image (512b, 521) from the user data (523) using the characteristic data (523, 517b) for use in establishing that the transaction was valid by associating the characteristic image with the transaction data.

2. A transaction processing system as claimed in claim 1 wherein the transaction terminal comprises means to establish that the user is authorised to effect the transaction.

3. A transaction processing system as claimed in claim 1 or claim 2 wherein the user data (523) comprises a random number combined with a digital representation (512a) of the characteristic image.

4. A transaction processing system as claimed in any preceding claim wherein the characteristic data (513a, 517a) is generated from the user data using a hashing algorithm.

5. A transaction processing system as claimed in any preceding claim wherein the transaction message (520) comprises a transaction portion containing the transaction data (514) and a seal portion, the seal portion comprising the characteristic data encrypted using a key (516) derived from the transaction data.

6. A transaction processing system as claimed in claim 5 wherein the key (516) is derived from the transaction data using a hashing algorithm.

7. A transaction processing system as claimed in any preceding claim wherein the data processing system comprises a first data processing facility (13) for use by a verifier, the first data processing facility comprising the means to rec ive from the network and store the transaction message (520) and means to effect the transaction using the transaction data; and a second data processing facility (14) for use by an arbiter, the second data processing facility

comprising means to store the user data; logic for recovering the characteristic data (517b) from th stored transaction m ssage (520) using the transaction data (514); and logic for reconstructing the characteristic image (512b, 521) from the characteristic data (523, 517b) using the user data for use in establishing that the transaction was valid by associating the characteristic image with the transaction data.

8. Transaction processing system as claimed in claim 7 wherein the characteristic data (513a) is generated from the user data using a hashing algorithm and the first data processing facility comprises means for storing encrypted user data (523) encrypted using the characteristic data; logic for recovering the characteristic data (517b) from the stored transaction message (520) using the transaction data (514); logic (505b) for decrypting the encrypted user data using the recovered characteristic data (517b); logic (503c) for generating the characteristic data (513b) from the decrypted user data; and means (508) to compare the characteristic data generated from the decrypted user data with the recovered characteristic data to establish the validity of the transaction.

9. A transaction processing system as claimed in any preceding claim wherein the transaction terminal comprises a smart card (515) supplied by the user and a smart card reader, the smart card comprising means to store the characteristic data (517a) and logic for combining the characteristic data with the transaction data for use in generating the transaction message.

10. A transaction processing system as claimed in claim 9 wherein the smart card comprises means for storing a user-specific encryption key and logic for encrypting the characteristic data using the user-specific encryption key, the data processing system comprising means to store the user-specific key, and logic for using the user specific key to recover the characteristic data from the transaction message.

11. A transaction terminal adapted for use in a transaction processing system as claimed in any preceding claim.

12. A smart card adapted for use in a transaction terminal as claimed in claim 11 as dependent on claim 9 or claim 10.

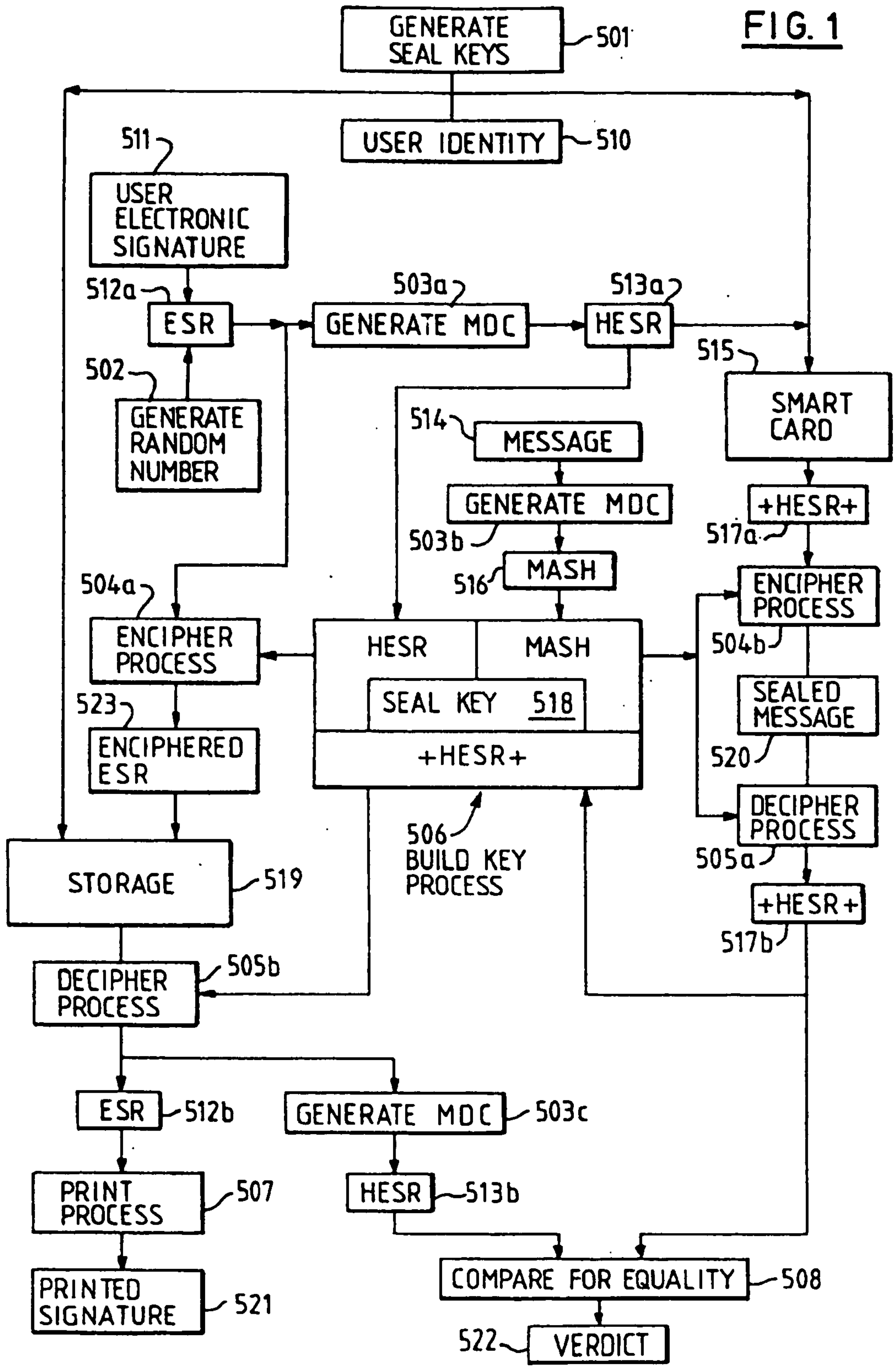
13. A data processing system adapted for use as the first data processing facility in a transaction processing system as claimed in claim 7 or claim 8.

14. A data processing system adapted for use as the second data processing facility in a transaction processing system as claimed in claim 7 or claim 8.

15. Apparatus for enrolling users of a transaction processing system as claimed in any of claims 1 to 10, the apparatus comprising: means to generate and store a digital representation (511) of the characteristic image for each user; and logic for generating the user data and the characteristic data (513a) from the digital representation of the characteristic image.

16. Apparatus as claimed in claim 15, the apparatus comprising logic (504a) for encrypting the user data using the characteristic data.

FIG. 1


GENERATE SEAL KEYS
501
USER IDENTITY
510
511
USER ELECTRONIC SIGNATURE
512a
ESR
502
GENERATE RANDOM NUMBER
503a
GENERATE MDC
513a
HESR
515
SMART CARD
514
MESSAGE
GENERATE MDC
503b
MASH
516
+HESR+
517a
ENCIPHER PROCESS
504b
504a
ENCIPHER PROCESS
HESR
MASH
SEAL KEY 518
+HESR+
SEALED MESSAGE
520
523
ENCIPHERED ESR
DECIPHER PROCESS
505a
+HESR+
517b
506
BUILD KEY PROCESS
STORAGE
519
DECIPHER PROCESS
505b
ESR
512b
GENERATE MDC
503c
PRINT PROCESS
507
HESR
513b
PRINTED SIGNATURE
521
COMPARE FOR EQUALITY
508
522
VERDICT

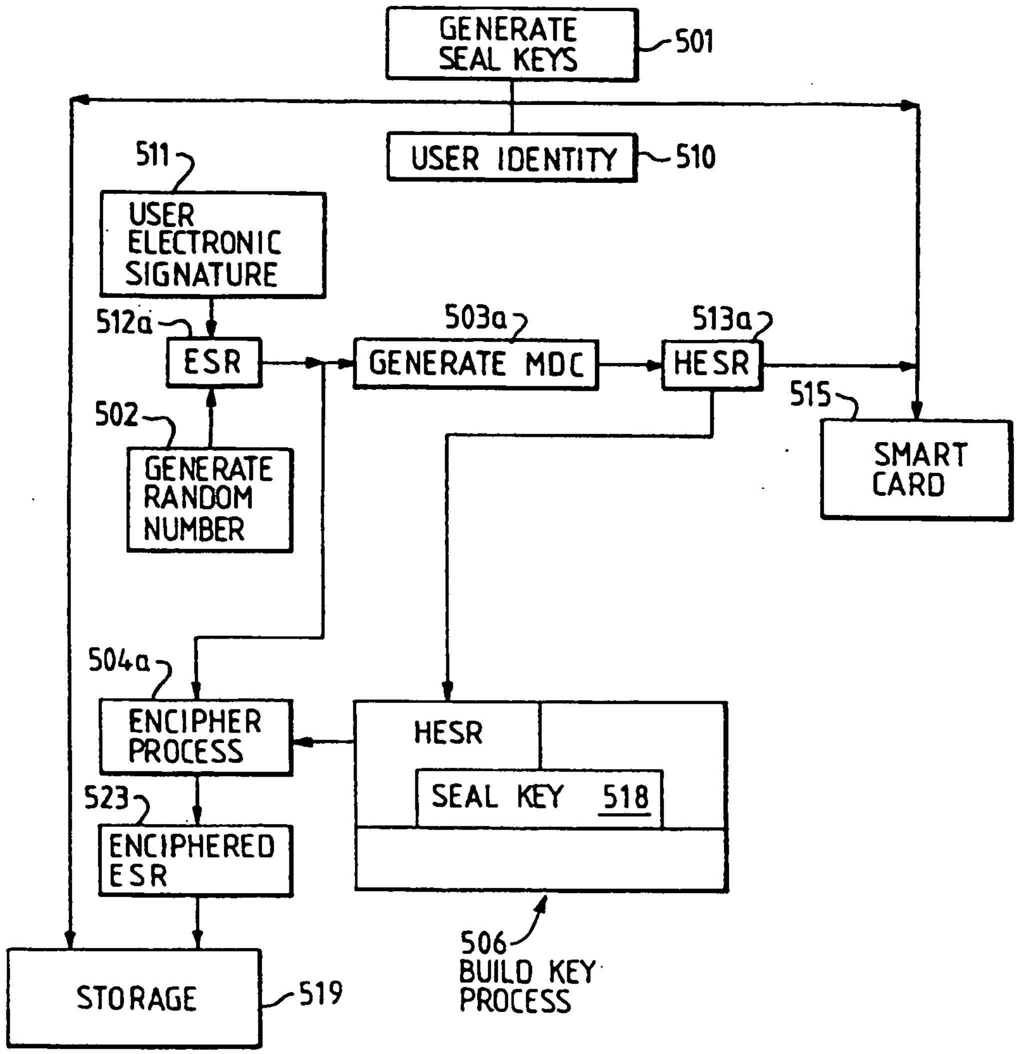

GENERATE SEAL KEYS
501
USER IDENTITY
510
511
USER ELECTRONIC SIGNATURE
512a
ESR
503a
GENERATE MDC
513a
HESR
515
SMART CARD
502
GENERATE RANDOM NUMBER
504a
ENCIPHER PROCESS
HESR
SEAL KEY 518
523
ENCIPHERED ESR
STORAGE
519
506
BUILD KEY PROCESS

FIG. 2

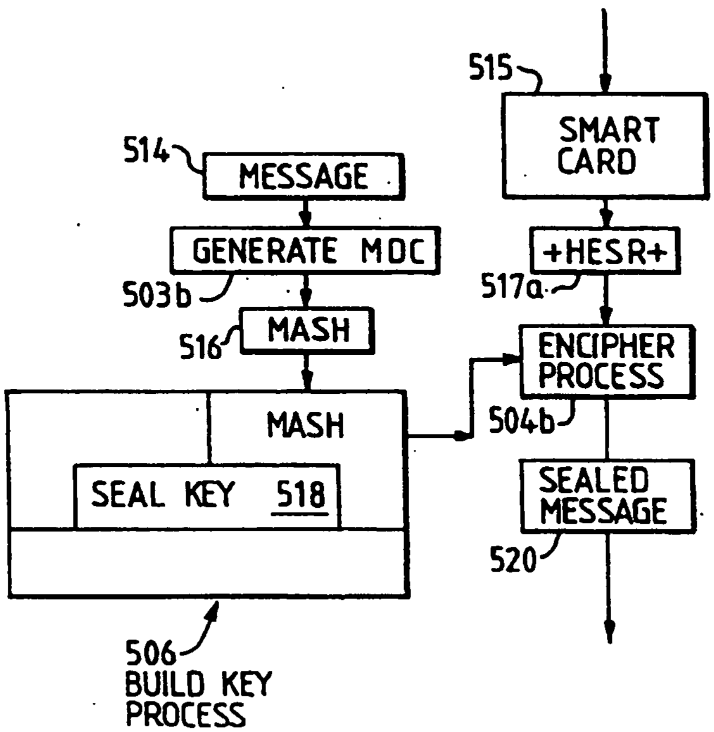

515
SMART CARD
514
MESSAGE
GENERATE MDC
503b
MASH
516
+HESR+
517a
ENCIPHER PROCESS
504b
MASH
SEAL KEY 518
SEALED MESSAGE
520
506
BUILD KEY PROCESS

FIG. 3

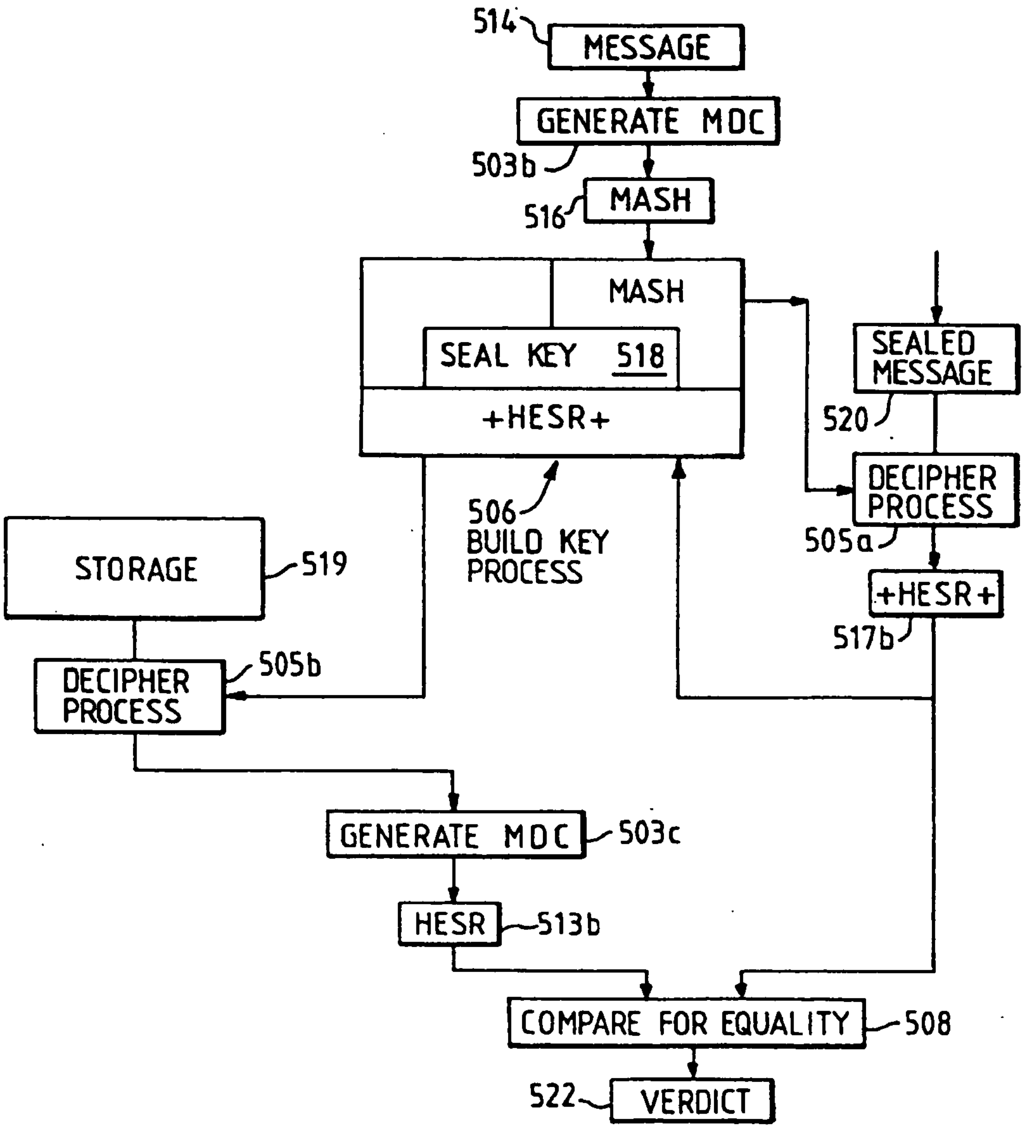

514
MESSAGE
GENERATE MDC
503b
MASH
516
MASH
SEAL KEY 518
+HESR+
506
BUILD KEY
PROCESS
SEALED
MESSAGE
520
DECIPHER
PROCESS
505a
+HESR+
517b
STORAGE
519
DECIPHER
PROCESS
505b
GENERATE MDC
503c
HESR
513b
COMPARE FOR EQUALITY
508
522
VERDICT

FIG. 4

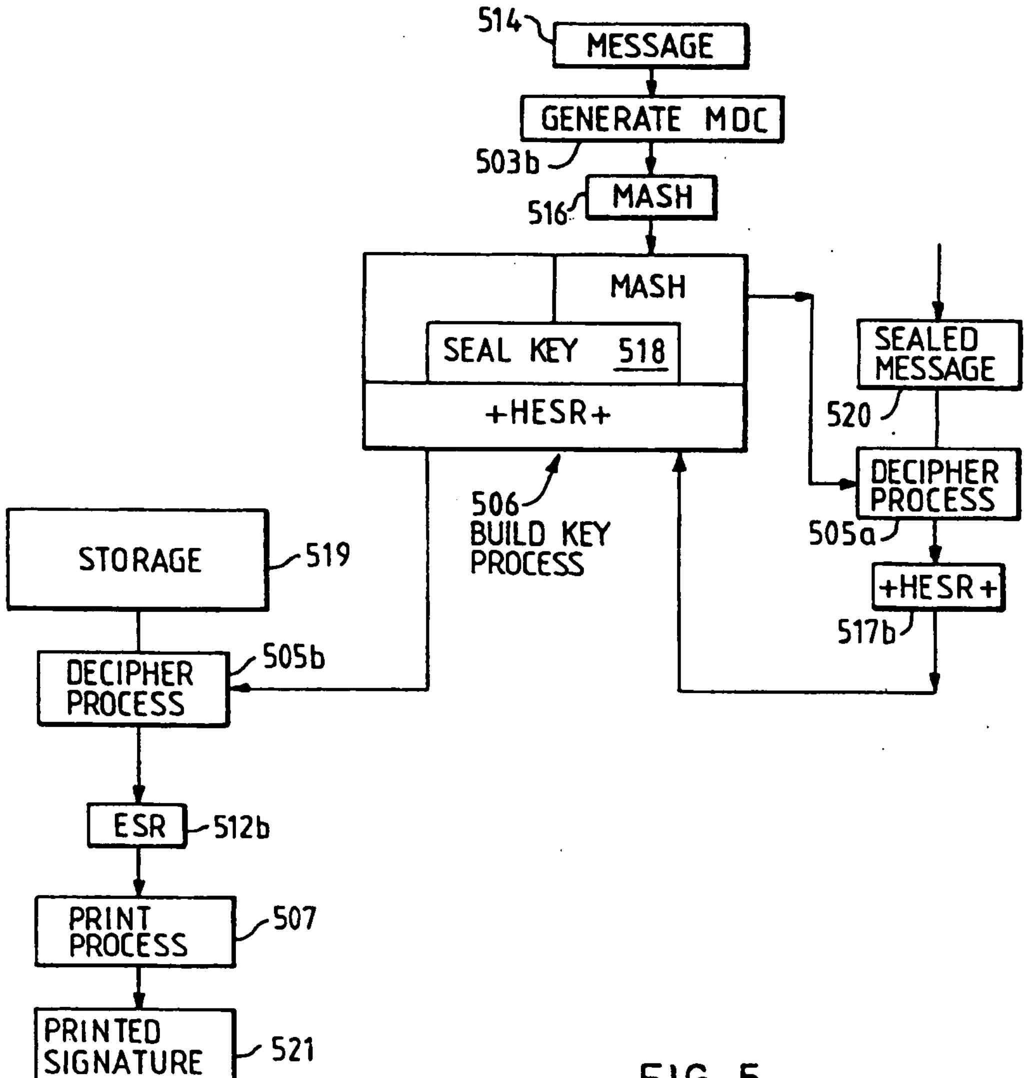

MESSAGE
514
GENERATE MDC
503b
MASH
516
MASH
SEAL KEY 518
+HESR+
506
BUILD KEY PROCESS
SEALED MESSAGE
520
DECIPHER PROCESS
505a
+HESR+
517b
STORAGE
519
DECIPHER PROCESS
505b
ESR
512b
PRINT PROCESS
507
PRINTED SIGNATURE
521

FIG. 5

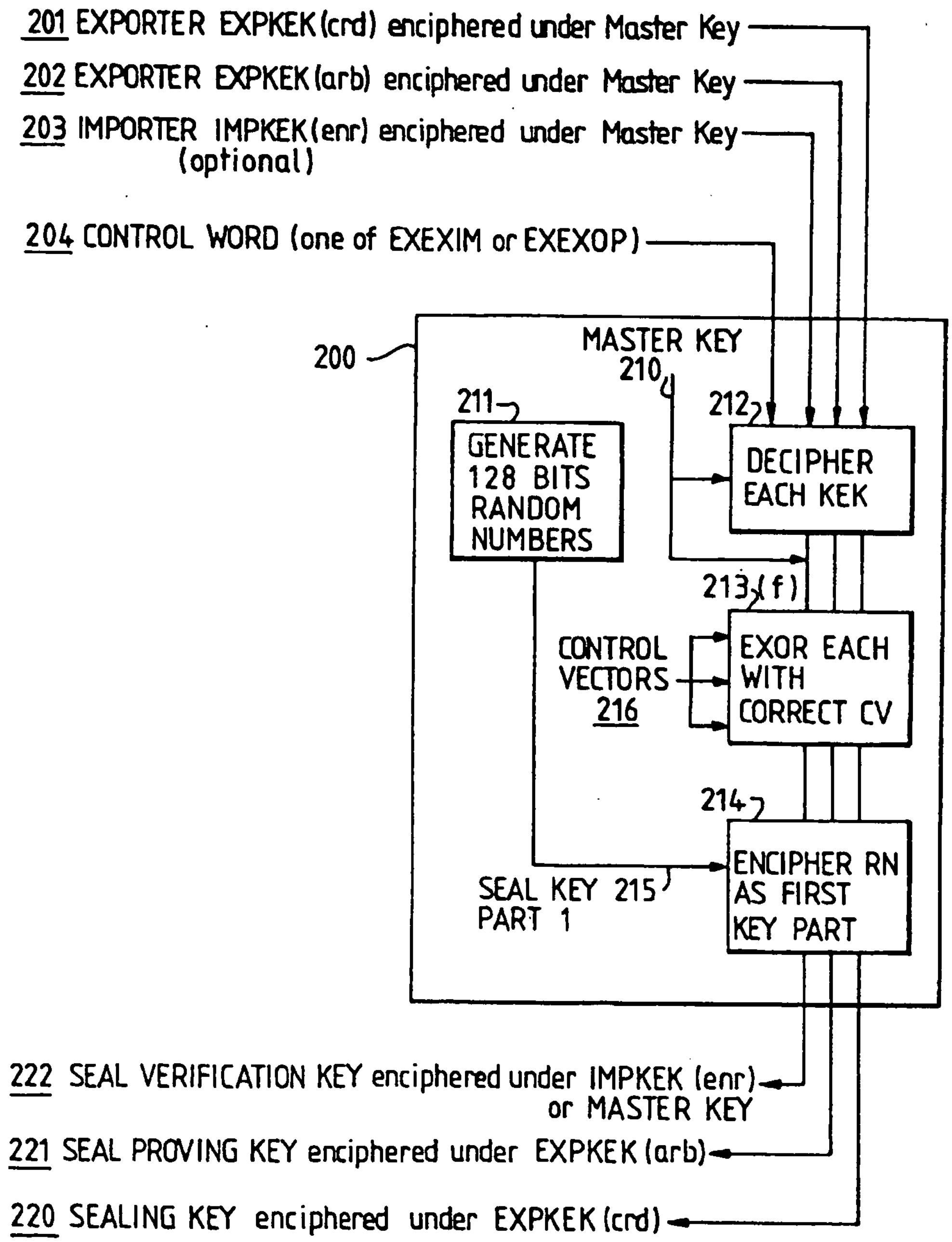

201 EXPORTER EXPKEK(crd) enciphered under Master Key
202 EXPORTER EXPKEK(arb) enciphered under Master Key
203 IMPORTER IMPKEK(enr) enciphered under Master Key (optional)
204 CONTROL WORD (one of EXEXIM or EXEXOP)
200
MASTER KEY 210
211
GENERATE 128 BITS RANDOM NUMBERS
212
DECIPHER EACH KEK
213 (f)
CONTROL VECTORS 216
EXOR EACH WITH CORRECT CV
214
SEAL KEY PART 1 215
ENCIPHER RN AS FIRST KEY PART
222 SEAL VERIFICATION KEY enciphered under IMPKEK (enr) or MASTER KEY
221 SEAL PROVING KEY enciphered under EXPKEK (arb)
220 SEALING KEY enciphered under EXPKEK (crd)

FIG. 6

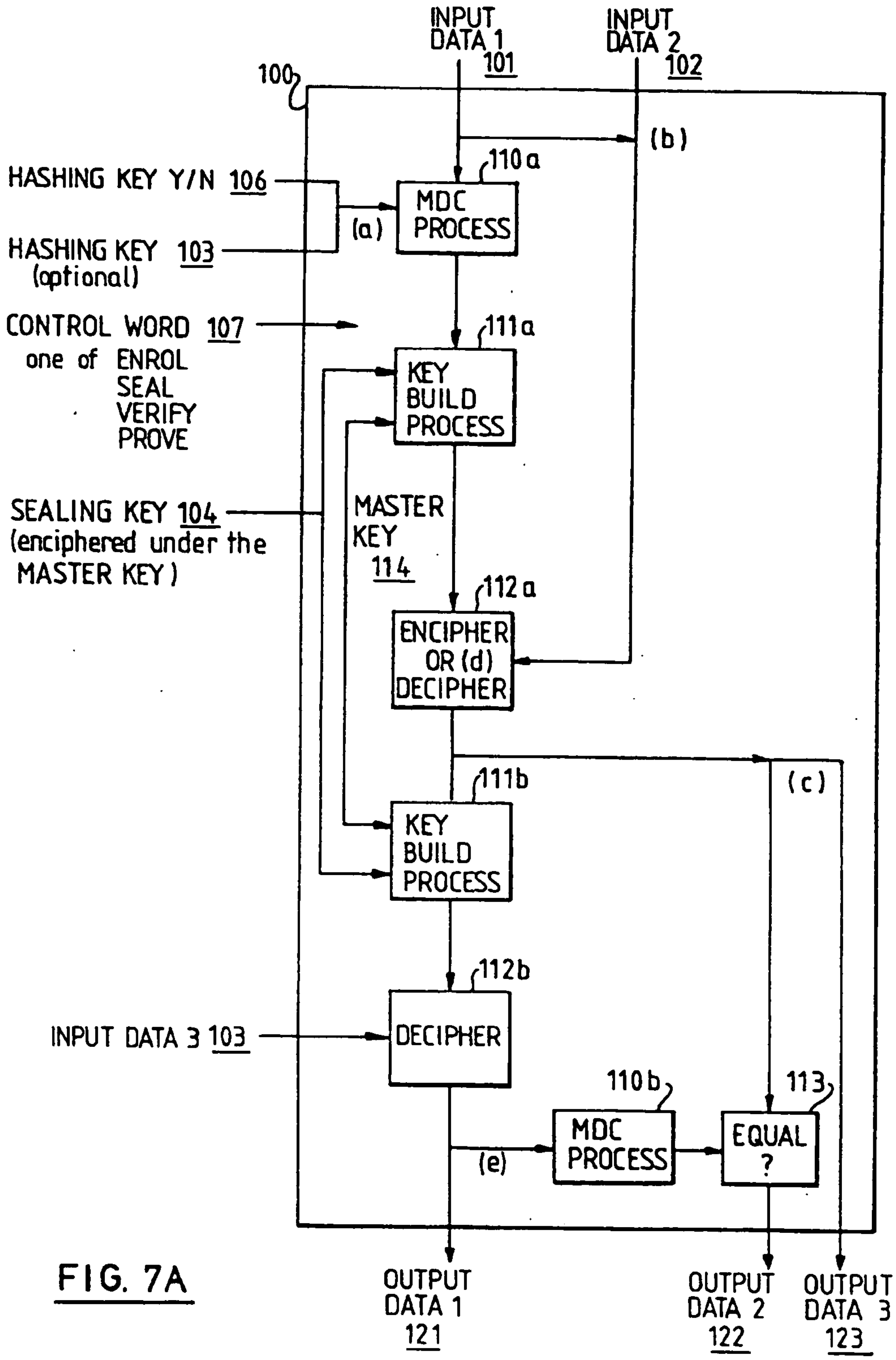

INPUT DATA 1 101
INPUT DATA 2 102
100
(b)
110a
HASHING KEY Y/N 106
MDC PROCESS
(a)
HASHING KEY 103 (optional)
CONTROL WORD 107
one of ENROL SEAL VERIFY PROVE
111a
KEY BUILD PROCESS
SEALING KEY 104 (enciphered under the MASTER KEY)
MASTER KEY 114
112a
ENCIPHER OR (d) DECIPHER
(c)
111b
KEY BUILD PROCESS
112b
INPUT DATA 3 103
DECIPHER
110b
113
MDC PROCESS
(e)
EQUAL ?
OUTPUT DATA 1 121
OUTPUT DATA 2 122
OUTPUT DATA 3 123

FIG. 7A

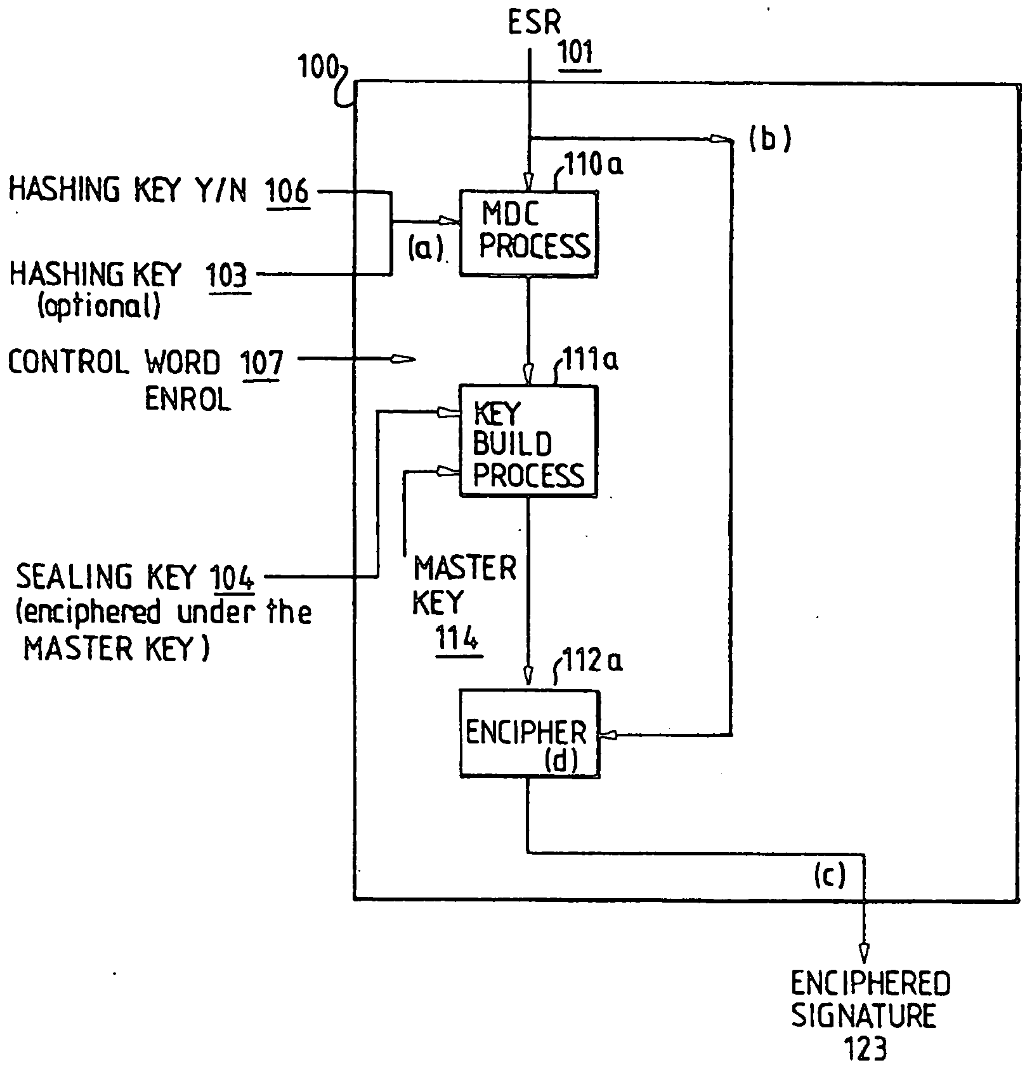

ESR
101
100
(b)
110a
HASHING KEY Y/N 106
MDC
PROCESS
(a)
HASHING KEY 103
(optional)
CONTROL WORD 107
ENROL
111a
KEY
BUILD
PROCESS
SEALING KEY 104
(enciphered under the
MASTER KEY)
MASTER
KEY
114
112a
ENCIPHER
(d)
(c)
ENCIPHERED
SIGNATURE
123

FIG. 7B

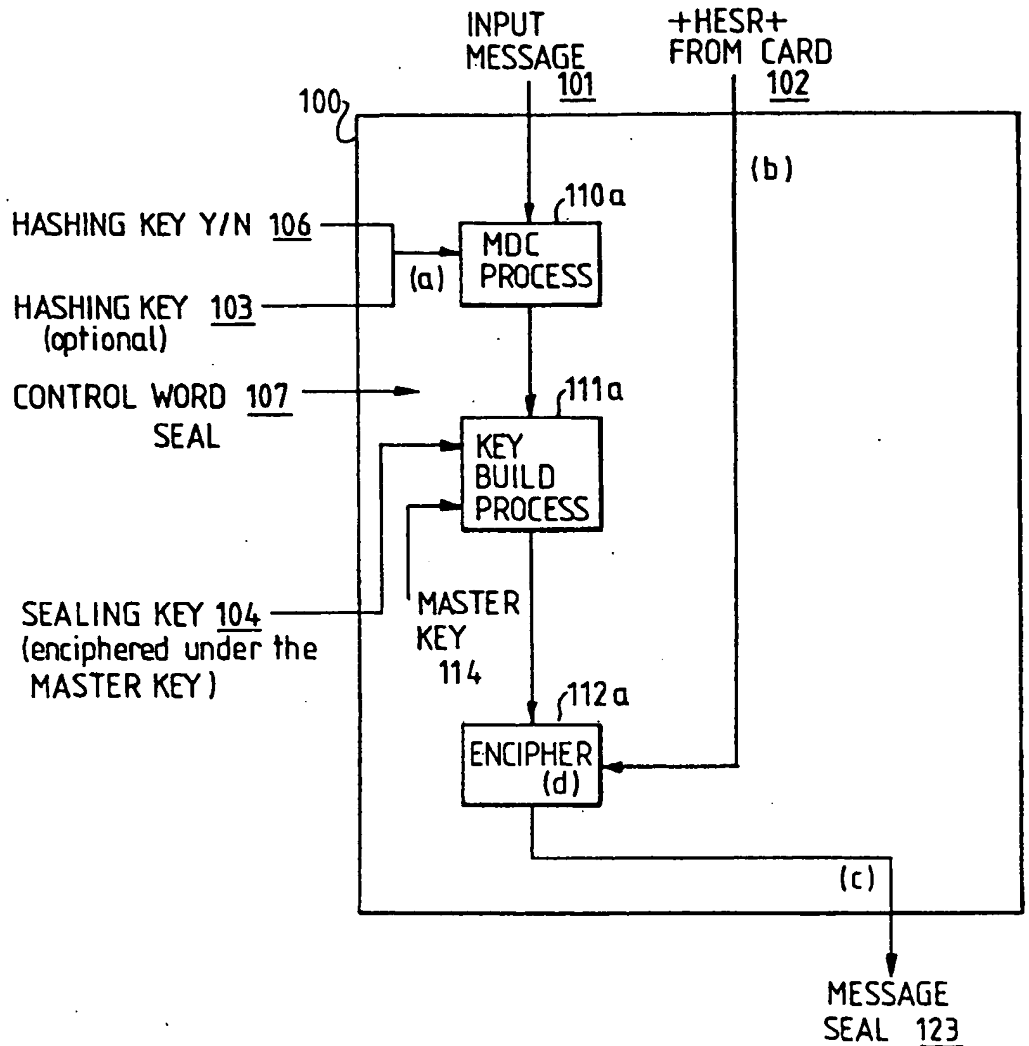

INPUT MESSAGE 101
+HESR+ FROM CARD 102
100
(b)
110a
HASHING KEY Y/N 106
MDC PROCESS
(a)
HASHING KEY 103 (optional)
CONTROL WORD 107 SEAL
111a
KEY BUILD PROCESS
SEALING KEY 104 (enciphered under the MASTER KEY)
MASTER KEY 114
112a
ENCIPHER (d)
(c)
MESSAGE SEAL 123

FIG. 7C

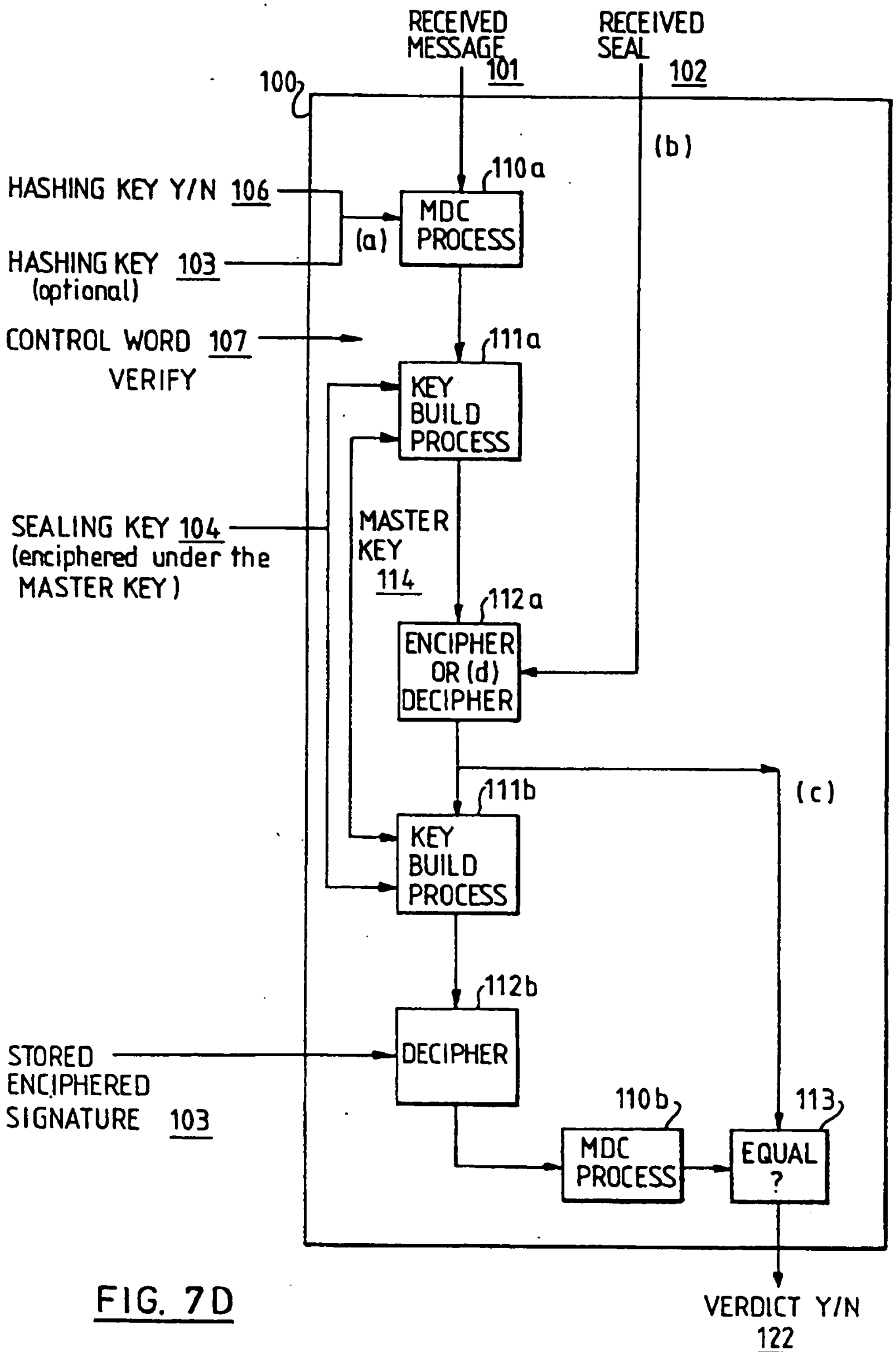

RECEIVED MESSAGE 101
RECEIVED SEAL 102
100
(b)
110a
HASHING KEY Y/N 106
MDC PROCESS
(a)
HASHING KEY 103 (optional)
CONTROL WORD 107
VERIFY
111a
KEY BUILD PROCESS
SEALING KEY 104 (enciphered under the MASTER KEY)
MASTER KEY 114
112a
ENCIPHER OR (d) DECIPHER
(c)
111b
KEY BUILD PROCESS
112b
STORED ENCIPHERED SIGNATURE 103
DECIPHER
110b
113
MDC PROCESS
EQUAL ?
VERDICT Y/N 122

FIG. 7D

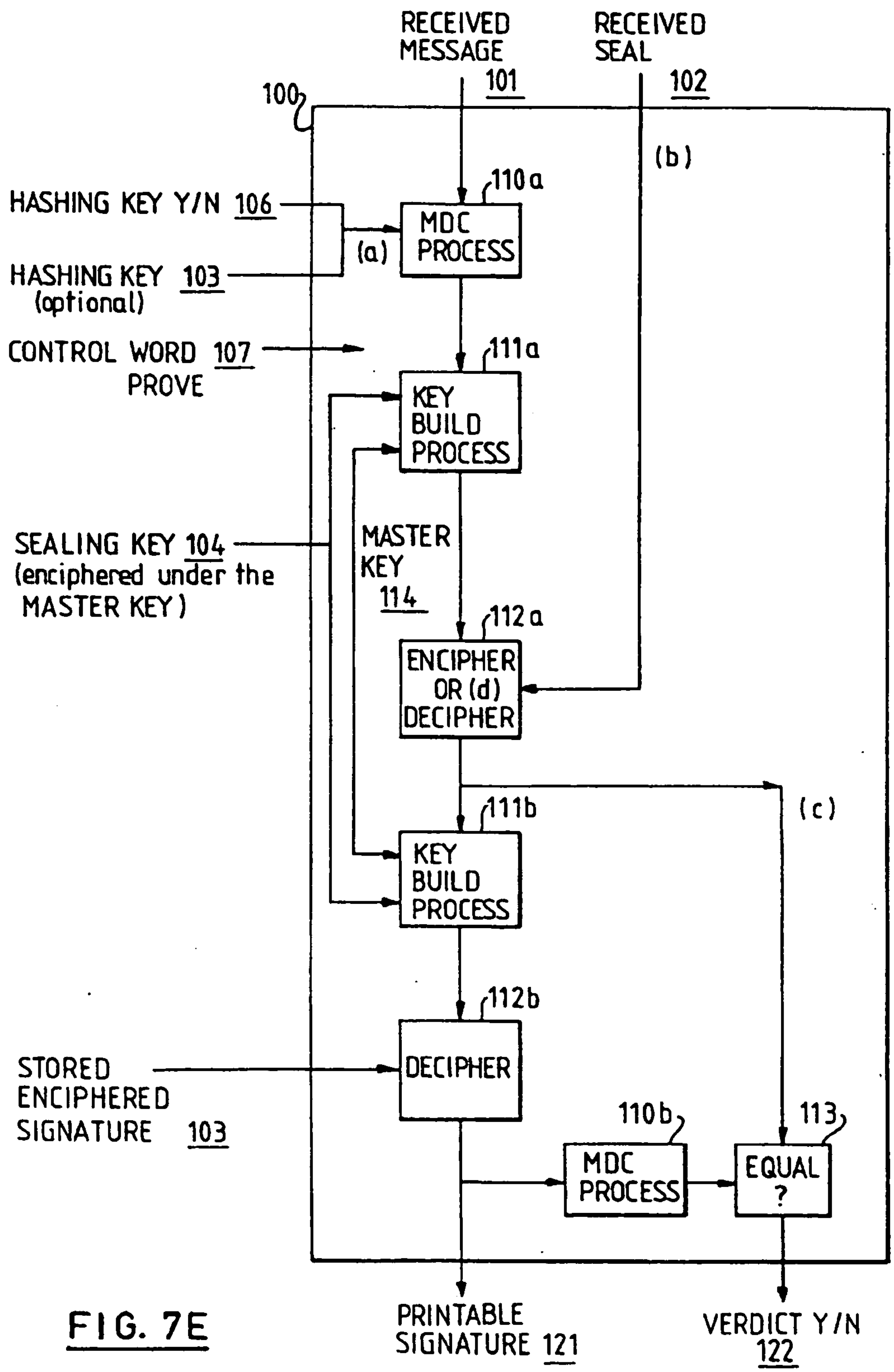

RECEIVED MESSAGE 101
RECEIVED SEAL 102
100
(b)
110a
HASHING KEY Y/N 106
MDC PROCESS
(a)
HASHING KEY 103 (optional)
CONTROL WORD 107 PROVE
111a
KEY BUILD PROCESS
SEALING KEY 104 (enciphered under the MASTER KEY)
MASTER KEY 114
112a
ENCIPHER OR (d) DECIPHER
111b
(c)
KEY BUILD PROCESS
112b
STORED ENCIPHERED SIGNATURE 103
DECIPHER
110b
113
MDC PROCESS
EQUAL ?
PRINTABLE SIGNATURE 121
VERDICT Y/N 122

FIG. 7E

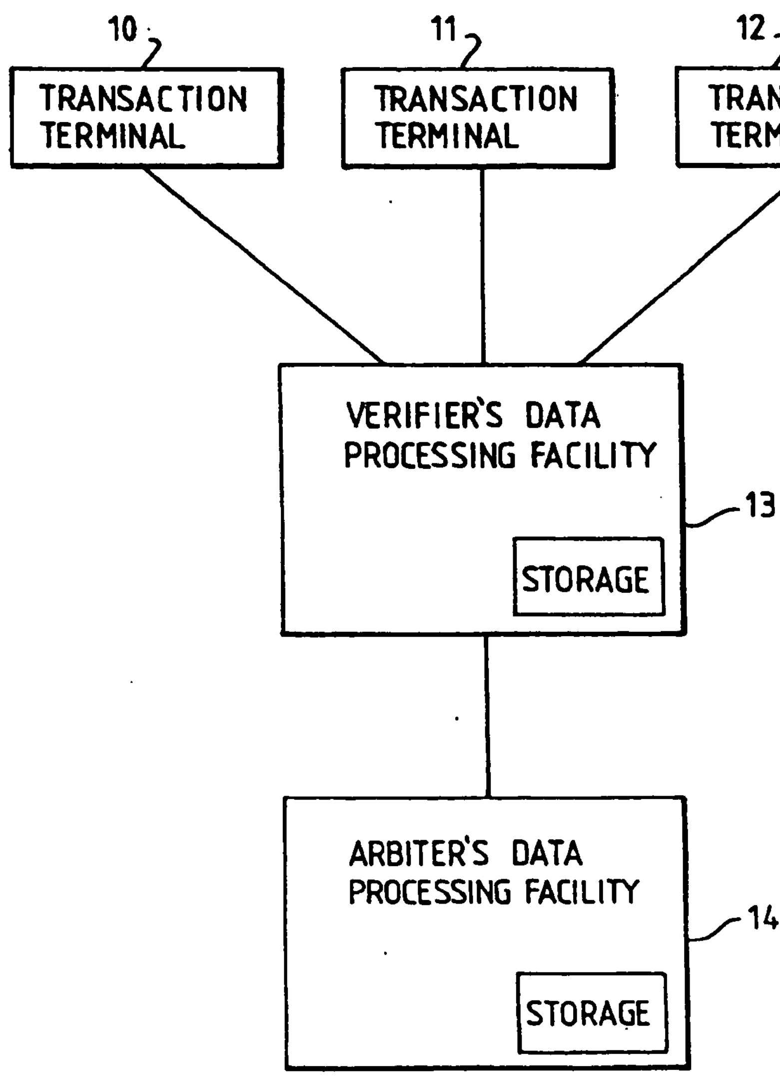

10
TRANSACTION TERMINAL
11
TRANSACTION TERMINAL
12
TRANSACTION TERMINAL
VERIFIER'S DATA PROCESSING FACILITY
STORAGE
13
ARBITER'S DATA PROCESSING FACILITY
STORAGE
14

FIG. 8

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 94306834.6

Category	DOCUMENTS CONSIDERED TO BE RELEVANT Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. 6)
Y	WO - A - 89/08 899 (DATACARD CORPORATION) * Claim 15; page 9, last sentence; page 10, lines 1-20; page 14, first chapter; page 15, last chapter; page 20, lines 22-35; fig. 1,5 *	1,2,3	G 07 F 7/12
A		7,9,11	
Y	WO - A - 91/10 207 (TEKNETRON COMMUNICATION SYSTEMS INC.) * Claims 1,4,19,24,25 *	1,2,3	
A		5	
A	US - A - 5 027 401 (SOLTESZ) * Column 4, first paragraph *	1,2,3	
A	EP - A - 0 334 616 (LEUGHTON, MICALI) * Claims 1,7 *	4,6,8, 10,12, 15,16	TECHNICAL FIELDS SEARCHED (Int. Cl.6) G 07 F G 09 C G 06 K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	16-12-1994	BISTRICH

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)